



UNITED STATES PATENT AND TRADEMARK OFFICE

UNITED STATES DEPARTMENT OF COMMERCE
United States Patent and Trademark Office
Address: COMMISSIONER FOR PATENTS
P.O. Box 1450
Alexandria, Virginia 22313-1450
www.uspto.gov

A

APPLICATION NO.	FILING DATE	FIRST NAMED INVENTOR	ATTORNEY DOCKET NO.	CONFIRMATION NO.
09/720,353	12/21/2000	Michael Nolte	6400-11WOUS	1134
7590	07/14/2005		EXAMINER	
McCormick Paulding & Huber City Place II 185 Asylum Street Hartford, CT 06103-4102			POLTORAK, PIOTR	
			ART UNIT	PAPER NUMBER
			2134	

DATE MAILED: 07/14/2005

Please find below and/or attached an Office communication concerning this application or proceeding.

Office Action Summary	Application No.	Applicant(s)
	09/720,353	NOLTE, MICHAEL
	Examiner Peter Poltorak	Art Unit 2134

-- The MAILING DATE of this communication appears on the cover sheet with the correspondence address --

Period for Reply

A SHORTENED STATUTORY PERIOD FOR REPLY IS SET TO EXPIRE 3 MONTH(S) FROM THE MAILING DATE OF THIS COMMUNICATION.

- Extensions of time may be available under the provisions of 37 CFR 1.136(a). In no event, however, may a reply be timely filed after SIX (6) MONTHS from the mailing date of this communication.
- If the period for reply specified above is less than thirty (30) days, a reply within the statutory minimum of thirty (30) days will be considered timely.
- If NO period for reply is specified above, the maximum statutory period will apply and will expire SIX (6) MONTHS from the mailing date of this communication.
- Failure to reply within the set or extended period for reply will, by statute, cause the application to become ABANDONED (35 U.S.C. § 133). Any reply received by the Office later than three months after the mailing date of this communication, even if timely filed, may reduce any earned patent term adjustment. See 37 CFR 1.704(b).

Status

- 1) Responsive to communication(s) filed on 08 April 2005.
- 2a) This action is FINAL. 2b) This action is non-final.
- 3) Since this application is in condition for allowance except for formal matters, prosecution as to the merits is closed in accordance with the practice under *Ex parte Quayle*, 1935 C.D. 11, 453 O.G. 213.

Disposition of Claims

- 4) Claim(s) 2-11 is/are pending in the application.
- 4a) Of the above claim(s) _____ is/are withdrawn from consideration.
- 5) Claim(s) _____ is/are allowed.
- 6) Claim(s) 2-11 is/are rejected.
- 7) Claim(s) _____ is/are objected to.
- 8) Claim(s) _____ are subject to restriction and/or election requirement.

Application Papers

- 9) The specification is objected to by the Examiner.
- 10) The drawing(s) filed on _____ is/are: a) accepted or b) objected to by the Examiner.
Applicant may not request that any objection to the drawing(s) be held in abeyance. See 37 CFR 1.85(a).
Replacement drawing sheet(s) including the correction is required if the drawing(s) is objected to. See 37 CFR 1.121(d).
- 11) The oath or declaration is objected to by the Examiner. Note the attached Office Action or form PTO-152.

Priority under 35 U.S.C. § 119

- 12) Acknowledgment is made of a claim for foreign priority under 35 U.S.C. § 119(a)-(d) or (f).
- a) All b) Some * c) None of:
 1. Certified copies of the priority documents have been received.
 2. Certified copies of the priority documents have been received in Application No. _____.
 3. Copies of the certified copies of the priority documents have been received in this National Stage application from the International Bureau (PCT Rule 17.2(a)).

* See the attached detailed Office action for a list of the certified copies not received.

Attachment(s)

1) <input type="checkbox"/> Notice of References Cited (PTO-892)	4) <input type="checkbox"/> Interview Summary (PTO-413)
2) <input type="checkbox"/> Notice of Draftsperson's Patent Drawing Review (PTO-948)	Paper No(s)/Mail Date. _____
3) <input type="checkbox"/> Information Disclosure Statement(s) (PTO-1449 or PTO/SB/08) Paper No(s)/Mail Date _____	5) <input type="checkbox"/> Notice of Informal Patent Application (PTO-152)
	6) <input type="checkbox"/> Other: _____

DETAILED ACTION

1. The Amendment, and remarks therein, received on 4/08/2005 have been entered and carefully considered.

Response to Amendment

2. Applicant's arguments have been carefully considered but they were not found persuasive.
3. As per claims 11 applicant argues that Deo does not teach a one-time encryption. The Deo HMAC generator derives hash values and does not create a signing key by means of one-time encryption as disclosed in claim 11.
4. The examiner points out that the exact claim language is as follows: "... using one of the sequence number and the shared main key to create a signing key by means of a one-time encryption...".
5. As per claim 5 applicant argues that *Hoffmann* discloses "random data generated by a random data generator" rather than a "sequence number produced by a pseudo-random generator".
6. The examiner points out that any data in computers is essentially a sequence number of 1s and 0s. Furthermore, random generators actually are pseudo-random generators since "it is impossible to produce something truly random on a computer" (*Schneier*, pg. 44). The examiner points to Bruce Schneier, who provides Donald Knuth's quotation of John von Neumann: "Anyone who considers arithmetical methods of producing random digits is, of course, in a state of sin" (*Schneier*, pg. 44). As a result, one or more sequence numbers

(random data Z) that is generated by a random data generator as taught by *Hoffmann* (col. 3 lines 37-43) reads on a “sequence number produced by a pseudo-random generator. (For additional information the examiner points to the previous Office Action § 25.)

7. Applicant argues that the *Hoffmann* reference does not disclose an intermediate sender between the control center and receiver.
8. As per argument that *Hoffmann* does not disclose “causing the control center to produce one ore more sequence number” but rather *Hoffmann* teaches the generation of random data at the transmitter the examiner points to paragraph 6 above.
9. As per argument that the transfer key disclosed by *Hoffmann* is not involved in creating the signing key, instead *Hoffmann* discloses use of the transfer key to encipher and decipher random data the examiner points to *Hoffmann* who discloses in col. 1 lines 44-46 and col. 3 lines 19-22 that the signing key forms a signature for a message.
10. As per argument that a control center and a receiver don’t share a main key the examiner points to the previous Office Action, where the examiner shows the control center sending the main key to the receiver upon which both the control center and the receiver share the main key.
11. As per claim 9 applicant argues the examiner’s position that the control center and the receiver inherently comprise memory is incorrect, and as an example applicant provides a building.

12. Applicant's argument is not understood. One of ordinary skill in the art would

have recognized that *Hoffmann*'s teaching refers to entities involved in electronic data transactions (sending and receiving electronic data) and as a result one of ordinary skill in the art would have found unreasonable to assume that either the control center or the receiver taught by *Hoffmann* could be a building.

13. As per claim 9, applicant contest the inherency of a one-time encrypter

connected to memory and another to a generator for a sequence number.

14. The examiner points that the sequence numbers and the common main key

(coupling data K) creating a signing key (symmetric key E) by means of one-time encryption (col. 3 lines 37-43), the process that in computer science does require memory. Even if the random data was entered manually into the enciphering process as hypothesized by applicant, one of ordinary skill in the art would have realized that *Hoffmann*'s invention is not a purely mechanical device and as a result one of ordinary skill in the art would have expected some input output means (*requiring memory for data input/output processing*) to receive manually entered data.

15. Applicant argues that *Hoffmann* lacks disclosure of "a device, which

assembles at least the signature and the message".

16. The examiner points to Fig. 2 that illustrates the signature assembled with the

message. Once again one of ordinary skill in the art would realized that the manual assembling, although theoretically possible, would involve computing devices.

17. Similarly, applicant argues on the same ground the other limitations in claim

9. Referring to Fig. 4 presented by *Hoffmann*, applicant argues that

Hoffmann does not show a signature checker provided in the receiver having inputs connected to the message".

18. The examiner points to Fig. 2 wherein *Hoffmann* clearly shows that a

message is an input to the receiver, which includes a signature checker.

19. In regard to claim 8 applicant argues the previous Office Action rejection

underling that *Horstmann* does not teach a receiver.

20. The examiner reminds applicant that claim 8 is rejected over *Hoffmann* in

view of *Horstmann*. *Hoffmann* teach a receiver where the *Horstmann*

reference is primarily used to provide teaching of a list of already used

sequence numbers (see the previous Office Action, § 31). Furthermore, it is

clear from a Fig. 1 (*Horstmann*) that the clearinghouse is a receiver.

21. Lastly, in reference to claim 10, wherein applicant did not find motivation to

combine, the examiner points to the previous Office Action, § 31, wherein the

examiner takes an Official Notice that it is old and well-known practice to use

deterministic methods to produce numbers for benefit of having control over

number generation wherein given the same input the same output could be

generated.

22. Claims 2-11 have been examined.

23. The text of those sections of Title 35, U.S. Code not included in this action

can be found in a prior office action.

24. Claims 2-8 and 11 are rejected under 35 U.S.C. 112, second paragraph, as being indefinite for failing to particularly point out and distinctly claim the subject matter that applicant regards as the invention.

25. "Initializing" a control center and a receiver with a shared main key in claim 11 is not understood. The specification does not provide any teaching on the intended meaning and especially there is no "initializing" phrase used in regard to the receiver, the examiner assumes that the initialization with a shared main key is equivalent to making the shared main key available to a control center.

26. Claims 2-8 are rejected by the virtue of their dependence.

27. Claims 2-7, 9 and 11 remain rejected under 35 U.S.C. 102(b) as being anticipated by *Hoffmann et al.* (U.S. Patent No. 5608800).

28. As per claim 11 *Hoffmann et al.* teach a control center producing one or more sequence numbers (*random data Z*), and using one of the sequence numbers and the common main key (*coupling data K*) creating a signing key (*symmetric key E*) by means of one-time encryption (col. 3 lines 37-43). The signing key and the sequence number is provided to the sender via a secure transmission (a control center and a sender are both within a transmitter) and the sender using the signing key forms a signature for a message (col. 1 lines 44-46 and col. 3 lines 19-22). Furthermore *Hoffman et al.* teach a control center sharing undiscoverable main key with a receiver as well as sending the message to the receiver via a data set containing at least the message and

the (*enciphered*) signature (S/E) (col.3 lines 45-52). *Hoffman et al.* teach determining the sequence number from the received data set (col. 3 lines 65-67), passing the sequence number through a one-time encryption to produce a check key (col. 4 lines 1-3) and using the check key to verify the signature of the message (col. 4 lines 4-7).

Fig. 2 shows teach the sender sending the message to the receiver via the data set containing at least the message and the signature.

29. *Hoffman et al.* teach the limitation of claim 5 in col. 3 lines 37-38.

30. Claims 2-7 are substantially equivalent to the limitations of claim 11; therefore claims 2-7 are similarly rejected.

31. As per claim 9 the control center and the receiver inherently use memory.

Any data operation includes memory, and inputs as well as outputs of data or mechanisms operating on data are connected to memory. Furthermore

Hoffman et al. teach generator generating a sequence number (col. 3 lines

35-36) and the sequence number is used to generate a signing key

(*symmetric key*) using one-way enciphering, which reads on one input of a

first one-time encrypter being connected to a generator for a sequence

number: One-time encrypter generates the signing key that is used to create

a signature which is sent from the sender to the receiver (*refer to arguments*

per claim 11), which reads on an output of the one-time encrypter being

connected to the sender via a transport medium. Signature generator is

inherently connected to the output of the one-time encrypter (*output, that is*

the signing key) and to the message to be signed. *Hoffman et al.* teach data

message block (*message*) being sent from the sender to the receiver (col. 3 lines 49-52), which reads on an output of the signature generator being connected to a device which assembles at least the signature and the message to form a data message block and whose output is connected to the receiver via a transport medium. Fig. 4 shows a signature checker having input connected to the message and to the signature and an output of a second one-time encrypter and the input of the second one-time encrypter being connected to a means for providing a sequence number.

32. Claim 8 remains rejected under 35 U.S.C. 103(a) as being unpatentable over *Hoffmann et al.* (U.S. Patent No. 5608800) in view of *Horstmann* (U.S. Patent No 6009401).

33. As per claim 8 *Hoffmann et al.* teach the receiver as discussed above. *Hoffmann et al.* does not explicitly teach the receiver maintaining a list of already used sequence numbers, and rejects already used sequence numbers. *Horstmann et al.* teach a receiver (*the clearinghouse*) maintaining a list of already used sequence numbers (*used tickets*) and rejects already used sequence numbers (*Horstmann et al.*, col. 5 lines 21-27).

It would have been obvious to one of ordinary skill in the art at the time of applicant's invention to maintain a list of already used sequence numbers by a receiver and reject already used sequence numbers as taught by *Horstmann et al.*. One of ordinary skill in the art would have been motivated to perform such a modification in order to avoid a replay attacks (*Horstmann et al.*, col. 5 line 22-23).

34. Claim 10 remains rejected under 35 U.S.C. 103(a) as being unpatentable over *Hoffmann et al.* (U.S. Patent No. 5608800) in view of *Official Notice*.

35. *Hoffmann et al.* teach random number generator as discussed above.

Hoffmann et al. do not teach the generator producing a sequence number using a deterministic method. Official Notice is taken that it is old and well-known practice to use deterministic methods to produce numbers.

It would have been obvious to one of ordinary skill in the art at the time of applicant's invention to use deterministic methods to produce numbers. One of ordinary skill in the art would have been motivated to perform such a modification in order to have control over number generation wherein given the same input the same output could be generated.

Conclusion

Applicant's amendment necessitated the new ground(s) of rejection presented in this Office action. Accordingly, **THIS ACTION IS MADE FINAL**. See MPEP § 706.07(a). Applicant is reminded of the extension of time policy as set forth in 37 CFR 1.136(a).

A shortened statutory period for reply to this final action is set to expire THREE MONTHS from the mailing date of this action. In the event a first reply is filed within TWO MONTHS of the mailing date of this final action and the advisory action is not mailed until after the end of the THREE-MONTH shortened statutory period, then the shortened statutory period will expire on the date the advisory action is mailed, and any extension fee pursuant to 37 CFR 1.136(a) will be calculated from the mailing date of the advisory action. In no event, however, will

the statutory period for reply expire later than SIX MONTHS from the date of this final action.

Any inquiry concerning this communication or earlier communications from the examiner should be directed to Peter Poltorak whose telephone number is (571)272-3840. The examiner can normally be reached Monday through Thursday from 9:00 a.m. to 4:00 p.m. and alternate Fridays from 9:00 a.m. to 3:30 p.m.

If attempts to reach the examiner by telephone are unsuccessful, the examiner's supervisor, Gregory Morse can be reached on (571)272-3838. The fax phone number for the organization where this application or proceeding is assigned is 703-872-9306.

Information regarding the status of an application may be obtained from the Patent Application Information Retrieval (PAIR) system. Status information for published applications may be obtained from either Private PAIR or Public PAIR. Status information for unpublished applications is available through Private PAIR only. For more information about the PAIR system, see <http://pair-direct.uspto.gov>. Should you have questions on access to the Private PAIR system, contact the Electronic Business Center (EBC) at 866-217-9197 (toll-free).

Pelt
7/8/05

Gregory Morse
GREGORY MORSE
SUPERVISORY PATENT EXAMINER
TECHNOLOGY CENTER 2100